

ABSTRACTDISASSEMBLING OBJECT CODE

A method of disassembling object code to generate the original source code is discussed, together with a lister for performing the disassembly. The object code has relocation sections associated with some of the section data. For each location in the section data the lister determines if there is an associated relocation instruction and if there is, the lister derives certain additional information concerning the section data. The lister then generates the original source code, including the additional information.

One example of the additional information is an arithmetic expression used to calculate a value in a relocation instruction. The set of relocations associated with the location of the instruction are read in turn by the lister and by using an expression calculator and an expression stack, the original arithmetic expression can be reconstructed.